Strong Authentication at Fermilab

Quick Reference Card

Fermilab Computing Division - http://www.fnal.gov/cd/
Strong Authentication Documentation at:
http://www.fnal.gov/docs/strongauth/
Quick Reference Card last updated: 06/04/02

Connect via Kerberized Network Program from UNIX

The Kerberized network connection programs are located in /usr/krb5/bin. These programs MUST NOT prompt for or accept a Kerberos password. Authenticate on your desktop machine before connecting to remote host!

telnet	**% telnet [options] <host>** Useful Kerberos options (for telnet, rsh and rlogin): **-f** forward existing ticket to host **-F** make forwarded ticket re-forwardable to other hosts **-k <REALM>** specify realm in which to request ticket **-l <username>** specify username on host when different from that on source machine **-N** turn off ticket-forwarding **-x** turn on encryption
rsh	**% rsh <host> [options] <command>** Useful options: See telnet
rlogin	**% rlogin <host> [options]** Useful Kerberos options: See telnet
ftp	**% ftp [options] <host>** Useful Kerberos options: **-f** forward existing ticket to host **-n** disable auto-login; does authentication **-u** disable auto-login; no auto-authentication **protect level** (at **ftp>** propmt) set protection level (**safe** verifies checksum, **private** encrypts data)
rcp	**% rcp [options] <file1> <file2>** or **% rcp [options] <file> <directory>** Useful Kerberos options: **-F** forward existing ticket to host **-k <REALM>** specify realm in which to request ticket **-N** turn off ticket-forwarding **-x** turn on encryption
ksu	**% ksu [<target_user>]** Useful Kerberos options: **-n <target_principal>** target principal name Useful fact: Can ksu to self (**% ksu .**); no authentication or authorization takes place in this case.
ssh or slogin	**% ssh [options] <host> [<commmand>]** or **% slogin [options] <host>** Kerberized ssh (slogin) only! Otherwise you get CRYPTOCard prompt. Useful Kerberos options: **-k** turn off ticket-forwarding
scp	**% scp [options] <file1> <file2>** Kerberized scp only! Otherwise you get CRYPTOCard prompt.

Connect from Windows or Macintosh

WRQ is supported by CD at Fermilab, Windows Exceed 7 and Macintosh are not. Authenticate on your desktop machine before connecting to remote host!

Windows (WRQ)	Authenticate: **Start > Programs > Reflection > Utilities > Kerberos Manager > Authenticate** Connect via telnet: **Start > Programs > Reflection > Host - UNIX and Digital > File > Open** Connect via FTP: **Start > Programs > Reflection > FTP Client**
Windows (MIT Kerberos with Exceed 7)	Authenticate: **Start > Programs > Kerberos Utilities > Leash32 > Action > Get Ticket(s)** Connect via telnet: **Start > Programs > Hummingbird Connectivity v7.0 > HostExplorer > Telnet >** select session file **> Connect**
Macintosh (MIT Kerberos, unspecified network client; Newsflash: OS 10.1 kerberos preinstalled)	Authenticate: **Apple menu >Control Panels > Kerberos Control Panel >** select principal **> Get Tickets** Invoke telnet or FTP client to connect (product-dependent)

Connect from NonKerberized Machine: Portal Access

Portal access requires use of a CRYPTOCard (see back side). UNIX connection commands shown here.

ssh or slogin	**% ssh [options] <host>** or **% slogin [options] <host>** Give empty password at first prompt. CRYPTOCard supports **ssh** only when no command is given. Do not use **-f** and **-n**. Encryption set in config or via **-c <cipher>** option.
telnet	**% telnet [options] <host>** Unencrypted! Never type Kerberos password!
ftp	**% ftp [options] <host>** Unencrypted! Never type Kerberos password!
scp	**% scp [options] <file1> <file2>** Encryption set in config or via **-c <cipher>** option.

Manage Kerberos Tickets (UNIX)

These commands manage both Kerberos tickets and AFS tokens when AFS is installed (except kdestroy). Only authenticate or change password on local machine. If you MUST issue password over the network, verify that ALL connections in the chain are encrypted!

request tickets	default ticket options: **% kinit** forwardable: **% kinit -f** nonforwardable: **% kinit -F** renewable: **% kinit -r <lifetime>**
list tickets	showing flags: **% klist -f**
destroy tickets	**% kdestroy** Note: this does not destroy AFS token; to do so, use: **% unlog**

These commands manage both Kerberos tickets and AFS tokens when AFS is installed (except kdestroy). Only authenticate or change password on local machine. If you MUST issue password over the network, verify that ALL connections in the chain are encrypted!

renew tickets	UNIX: **% kinit -R** Using CRYPTOCard: **new-portal-ticket** On remote hosts: First renew tickets on local system, then run **k5push <host1> [<host2> ...]**

CRYPTOCard Use (Original Style Cards)

Warning! telnet sessions are not encrypted! Never type Kerberos password!

These instructions are for CRYPTOCards issued PRIOR TO March 2002.
Read the care and use instructions that come with your CRYPTOCard!
PIN length: 4 to 8 digits.
For all CRYPTOCard operations, use ON/OFF to turn the card on to begin, and (optionally) to turn it off when done.

Reset initial PIN	Enter initial PIN, press ENT At prompt “New PIN?”, enter new PIN, press ENT At prompt “Verify”, enter new PIN again, press ENT
Reset PIN (general)	Enter old PIN, press ENT At prompt “Fermilab”, press CPIN At prompt “New PIN?”, enter new PIN, press ENT At prompt “Verify”, enter new PIN again, press ENT
First use	(terminal) Run ssh, telnet, or ftp to Kerberized host (CRYPTOCard) Enter PIN, press ENT At prompt “Fermilab”, press ENT Press CH/MAC Enter challenge from computer screen into card Press ENT to generate response (terminal) Type response from CRYPTOCard
General use	(terminal) Run ssh, telnet, or ftp to Kerberized host (CRYPTOCard) Enter PIN, press ENT At prompt “Fermilab”, press ENT to get challenge Verify that challenges match Press ENT to generate response (terminal) Type response from CRYPTOCard
Reauthenticate	Type **new-portal-ticket** on terminal; follow “General use” instructions for CRYPTOCard starting with “Enter PIN”.
Resync Card	Follow procedure for “First use”.

CRYPTOCard Use (New Style Cards, 03/02)

Warning! telnet sessions are not encrypted! Never type Kerberos password!

These instructions are for CRYPTOCards issued starting in March 2002.
Read the care and use instructions that come with your CRYPTOCard!
PIN length: 4 to 8 digits.

Reset initial PIN	Press CHG PIN to turn on card At prompt “PIN?”, enter your initial PIN. At prompt “New PIN?”, enter new PIN, press ENT At prompt “Verify”, enter new PIN again, press ENT

These instructions are for CRYPTOCards issued starting in March 2002.
Read the care and use instructions that come with your CRYPTOCard!
PIN length: 4 to 8 digits.

Reset PIN (general)	Press CHG PIN to turn on card At prompt “PIN?”, enter old PIN, press ENT At prompt “New PIN?” enter new PIN, press ENT At prompt “Verify”, enter new PIN again, press ENT
First use	(terminal) Run ssh, telnet, or ftp to Kerberized host (CRYPTOCard) Press MENU to turn on card Enter PIN, press ENT Press MENU again (ignoring Adj LCD) At prompt “Resync” press ENT At prompt “Ready”, enter challenge from computer screen into card and press ENT (terminal) Type response from CRYPTOCard
General use (two methods)	1. (terminal) Run ssh, telnet, or ftp to Kerb’ed host (CRYPTOCard) Press PASSWORD to turn on card Enter PIN, press ENT At prompt “Fermilab”, press ENT Card now displays response, not the challenge! (terminal) Type response from CRYPTOCard 2. (terminal) Run ssh, telnet, or ftp to Kerb’ed host (CRYPTOCard) Press DIG SIG to turn on card Enter PIN, press ENT At prompt “Ready”, enter challenge from computer screen into card and press ENT Card now displays response (terminal) Type response from CRYPTOCard
Reauthenticate	Type **new-portal-ticket** on terminal; follow “General use” instructions for CRYPTOCard (omit “Run ssh, telnet, or ftp to Kerb’ed host”).
Resync Card	Follow procedure for “First use”.

Change Kerberos Password

In general, only change password on local machine. If you must issue password over the network, verify that connection is encrypted!

UNIX	**% kpasswd [<principal_name>]**
Windows (WRQ; recommended, CD-supported))	**Start > Programs > Reflection > Utilities > Kerberos Manager > Tools > Change Password...**
Windows (Kerb+Exceed 7; community-supported)	**Start > Programs > Hummingbird Connectivity v7.0 > HostExplorer > Telnet** Then run: **% kpasswd [<principal_name>]**
Macintosh (community-supported)	**Apple menu > Control Panels > Kerberos Control Panel >** select principal **> Get Tickets >** click on the ticket **> Change Password**

Common Error Messages

Messages shown in alphabetical order. Message in bold, causes/solutions in plain text underneath.

aklog: can't get afs configuration

(Users of ssh v1_2_27 or higher) Harmless but misleading. To get rid of, add **AFSRunAklog no** to /etc/sshd_config, restart sshd.

Cannot contact any KDC for requested realm

- Firewall blocks KDC request or reply
- DNS failure

Cannot establish a session with Kerberos administrative server ... preauthentication failed

Wrong password (most likely)

Incorrect net address

NAT or multiple-IP address host. Edit **[libdefaults]** in **krb5.conf**:

- UNIX: **proxy_gateway = <your fixed IP address>**
- Mac: **noaddresses = true**
- WRQ: no solution currently

KDC policy rejects request
KDC can't fulfill requested option

- Requesting a forwardable ticket for a /root or /admin instance
- Trying to forward an unforwardable ticket, or renew an unrenewable one

Key version number for principal in key table is incorrect

- Keytab has changed since service ticket was obtained; to solve, run **% kinit -R** or **% kinit**
- Service key in KDC was changed after keytab file was created; to solve, recreate keytab file on host

Preauthentication failed while getting initial credentials

- system clock error > 5 minutes
- wrong password
- user does not have a CRYPTOcard in the host's realm

Server not found in Kerberos database

- local hosts file or NIS map gives wrong name for host
- Bad or missing domain_realm mapping in /etc/krb5.conf
- Fermi Kerberos v1_2 bug; to solve, upgrade

WRQ error: **Preauthentication failed (KDC024)**

- Click **Help** for possible causes. Usually realm mismatch, wrong password or system clock error > 5 minutes